

Docket No.: 1509-482

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	
Maurizio PILU	:	Confirmation No.
U.S. Patent Application No.	:	Group Art Unit:
Filed:	:	Examiner:
For: IMAGE CAPTURE METHOD		

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claims, in the present application, the priority of GB Patent Application No. 0308393.8, filed April 11, 2003. The certified copy is submitted herewith.

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP



Randy A. Noranbrock
Registration No. 42,940
For Allan M. Lowe
Registration No. 19,641

1700 Diagonal Road
Alexandria, Virginia 22314
(703) 648-1111 AML/pjc
(703) 518-5499 Facsimile
Date: April 5, 2004

THIS PAGE BLANK (USPTO)



INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

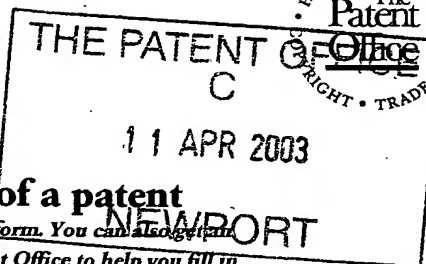
Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 3 February 2004



THIS PAGE BLANK (USPTO)



11 APR 03 E799464-1 D01463
P01/7700 0.00-0308393.8

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

11 APR 2003

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference 200207946-1 GB
2. Patent application number
(The Patent Office will fill in this part) 0308393.8
3. Full name, address and postcode of the or of each applicant (underline all surnames)
Hewlett-Packard Development Company, L.P.
20555 S.H. 249
Houston, TX 77070
USA

Patents ADP number (if you know it)

If the applicant is a corporate body, give the country/state of its incorporation

8557886001

4. Title of the invention Image Capture Method

5. Name of your agent (if you have one)

"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)

Bruce G R Jones
Hewlett-Packard Ltd, IP Section
Filton Road, Stoke Gifford
BRISTOL BS34 8QZ

Patents ADP number (if you know it)

8072258001

- | | | | |
|--|---------|---|--|
| 6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number | Country | Priority application number
(if you know it) | Date of filing
(day / month / year) |
|--|---------|---|--|

- | | | |
|---|-------------------------------|--|
| 7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application | Number of earlier application | Date of filing
(day / month / year) |
|---|-------------------------------|--|

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:

- a) any applicant named in part 3 is not an inventor, or
 - b) there is an inventor who is not named as an applicant, or
 - c) any named applicant is a corporate body.
- See note, (d))

Yes

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description

21

Claim(s)

9

Abstract

1

Drawing(s)

11 + 11

RM

10. If you are also filing any of the following, state how many against each item.

Priority documents

Translations of priority documents

Statement of inventorship and right to grant of a patent (*Patents Form 7/77*)

Request for preliminary examination and search (*Patents Form 9/77*)

1

Request for substantive examination (*Patents Form 10/77*)

Any other documents
(please specify)

Fee Sheet

11.

I/We request the grant of a patent on the basis of this application.

Signature

Date

Bruce Graeme Roland Jones 9 April 03

12. Name and daytime telephone number of person to contact in the United Kingdom

K Nommeots-Nomm Tel: 0117-312-9947

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.
- Write your answers in capital letters using black ink or you may type them.
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.
- If you have answered 'Yes' Patents Form 7/77 will need to be filed.
- Once you have filled in the form you must remember to sign and date it.
- For details of the fee and ways to pay please contact the Patent Office.

IMAGE CAPTURE METHOD

Field of the Invention

5 The present invention relates to the field of image capture.

Background to the Invention

10 Portable digital cameras have become miniaturized, and are becoming increasingly wide spread. Known mobile phone devices already have in built cameras, and picture messaging between mobile phones is an increasingly wide spread technology.

15 Further, wearable cameras are known, and have the potential for becoming widely used consumer products in the future.

20 For some persons, being included in photographs or picture messages when in public places has nuisance effect. Increasing usage of portable camera devices means that the privacy issue of capturing of images of subjects who would prefer not to be photographed is increased. Because portable cameras are small and may be unseen by a subject, in general persons cannot choose to avoid being in the field of view of a small portable camera and may have their pictures taken without their knowledge or consent.

25 The issue of privacy in relation to cameras is well known. Civil liberties organizations are known to campaign for the right for people not to be photographed or videod without their consent. However, with the widespread use of security cameras and other hand held portable camera devices, maintaining privacy from being photographed or video is becoming harder. Some security
30 companies market their products as 'privacy friendly' because they are supposed to retain only images containing faces of known individuals, typically, potential or actual criminals. In *'Privacy issues of wearable camera's -v- surveillance*

cameras' by Steve Mann – [HTTP://wearcam.org](http://wearcam.org), 1995, it is suggested that security camera or wearable cameras should be made visible, and that a wearable camera should have a visual indicator that it is active for capturing an image. This does not offer real privacy to individuals within the vicinity of the camera, but rather offers a chance to 'escape' from the field of view from a camera.

In JP 10031265 there is disclosed a device for preventing stealthy photographing in which a remote control receiver is provided for remote control in a camera, where the remote control receiver issues a warning sound when a camera captures an image. This does not prevent capture of a persons image, but rather alerts a person that a picture has been taken, or could be taken.

Further, there are known security systems which are able to detect and identify faces of known criminals from security video footage, such as those available from Identix, and Viisage, for example the known FaceFINDER product.

In US 20020039447, there is disclosed a system for indexing, storage and retrieval of digital images, whereby photographs are sorted according to who is in a photograph, through face recognition algorithms.

In US 20010016820, there is disclosed a face identification system, whereby faces are removed from a memory device, having been identified.

In JP 2001235812 there is disclosed an image processing method in a digital photographic processing device in which a digital processing device is provided with a masking pattern which can be super imposed on a portion of an image for obscuring that portion of the image. Control of the masking process lies with the operator of the photographic processing device, and a person whose image has been captured by the device has no control over the processing of the image or whether the image can be captured or not.

The Imageld company www.imageID.com has a known product, whereby a user can wear a tag. The tags are recognized by cameras and can be used to sort out images of people. The system recognizes and reads a set of markings within an image, and then sorts and stores matching identification codes in a database.

In US 6,067,399 there is disclosed a privacy mode for cameras and camcorders. Images of persons faces recorded on a camera or camcorder may be detected and obscured. In US 6,067,399 the person whose image is being captured has no control over whether a privacy mode of a camera or camcorder apparatus is set or not, but rather an operator of a camera/camcorder can determine the privacy mode. Therefore, privacy is not in the control of a person who's image is being captured.

In JP 2001313006, there is disclosed a method and apparatus in which a person carries a portable device which emits infra-red light which 'floods' a camera's sensors or film, thereby blanking the image. However, the method disclosed in JP 2001313006 disables image capture completely and inhibits all images being taken, within range of the device.

Summary of the Invention

According to a first aspect there is provided a method for modifying a captured image of a scene, said method comprising:

detecting an inhibit signal emanating from an inhibitor device carried by a person within said scene;

in response to said inhibit signal;

identifying a portion of said image corresponding to said person; and

modifying said image of said scene so as to obscure said image portion of said person.

Other aspects of the invention are as described in the claims herein.

5

Brief Description of the Drawings

For a better understanding of the invention and to show how the same may be carried into effect, there will now be described by way of example only, specific embodiments, methods and processes according to the present invention with reference to the accompanying drawings in which:

10

Figure 1 illustrates schematically a first embodiment image capture system comprising an image capture device, and at least one inhibitor device for controlling operation of the image capture device for taking images of a host wearer of the inhibitor device.

15

Fig. 2 illustrates schematically an omni-directional communication between an inhibitor device and an image capture device of the system of Fig. 1 herein;

Fig. 3 illustrates schematically a second embodiment image capture system, in which communication between an image capture device and an inhibitor device in which the image capture detects the inhibitor device using a directional receiver beam;

20

Fig. 4 illustrates schematically the inhibitor device and camera device of Fig. 3, in which the image capture device points in a direction away from the inhibitor device;

25

Fig. 5 illustrates schematically a scenario of two inhibitor devices and a single image capture device, the inhibitor device being in a field of view of the image capture device;

30

Fig. 6 illustrates schematically an example of an image captured by an image capture device before image processing is applied;

5 Fig. 7 illustrates schematically the image of Fig. 6, after image processing is applied to modify the image taking account of inhibitor devices within a field of view of the image capture device;

10 Fig. 8 illustrates schematically components of one specific implementation of an inhibitor device;

Fig. 9 illustrates schematically components of a specific implementation of an image capture device;

15 Fig 10, illustrates schematically a scenario in which an image capture device captures an image in a field of view which includes users wearing first and second inhibitor devices, and the image capture device recognizes one of the inhibitor devices;

20 Fig, 11 illustrates schematically processes carried out at image capture device, for recognizing an inhibitor device;

Fig. 12 illustrates schematically a signal processing channel within an image capture device;

25 Fig. 13 illustrates schematically communication between an image capture device and a remote third party, for obtaining authorization for decoding a portion of a captured image; and Fig 14 is a schematic illustration of an image captured device, an inhibitor and a trusted third party.

30 **Detailed Description of a Specific Mode for Carrying Out the Invention**

There will now be described by way of example only a specific mode contemplated by the inventors. In the following description numerous specific

details are set forth in order to provide a thorough understanding. It will be apparent however, to one skilled in the art, that the present invention may be practiced without limitation to these specific details. In other instances, well known methods and structures have not been described in detail so as not to
5 unnecessarily obscure the description.

In this specification, the term 'scene image', relates to an electronic image of a scene, and includes both a still image, and a video sequence.

10 In this specification, the term 'image capture device' relates to any device capable of capturing an image, and includes but is not limited to digital still cameras, and video cameras.

Specific implementations describe presentation of a person's image being
15 made available to an image capture device, particularly although not exclusively a portable image capture device, without their consent.

In one implementation, there is provided a wearable device which broadcasts an inhibit message in an area immediately surrounding a host wearer
20 of the device. Any portable image capture devices, such as cameras or the like of third parties within range of the device may receive the inhibit message, and in response to receiving the inhibit message, inhibit capture and/or apply processing of an image or part of an image.

25 Referring to Fig. 1 herein, there is illustrated schematically an inhibitor device 100 and an image capture device 101 in close proximity, in which the inhibitor device broadcasts an inhibit signal carrying an image capture inhibitor message. Camera device 101, may pick up the signal carrying the inhibit message. On receiving the inhibit message, the image capture device may react
30 in various ways.

In one mode of operation, the image capture device is permitted to capture an image of a scene, which may include a host wearer of the inhibitor device. However, the image capture device is unable to print or store a portion of the captured scene image which corresponds to a wearer of the inhibitor device.

5 Data processing components within the image capture device modify the scene image by identifying areas of the scene image which relate to a person wearing an inhibitor device, and obliterating selected parts of the image of the wearer of the inhibitor device. The selected parts of the image which are obliterated may comprise facial features in particular, but may also include items of clothing.

10

Some specific implementations described herein operate such that images which contain people who prefer not to have their images captured are automatically and forcefully modified before viewing, and in some implementations before storage; such that images of such persons are no longer

15 recognizable in the captured image. Suitably, only the portion of an overall image which relates to a person who requires privacy is obliterated from the image, leaving the remainder of the overall image intact.

20

The inhibitor device may send an inhibit message either omni-directionally, or directionally. The image capture device may receive one or more inhibit messages at the same time, either omni-directionally, or directionally.

25

The inhibit message may be carried on a signal carrier including but not limited to an ultrasonic signal carrier; a microwave signal carrier; a radio frequency signal carrier; a visual light signal, or an infrared light signal.

30

In the second mode of operation an inhibit signal generated from a position within a field of view of an image capture device is identified, and its position within a capture image taken of that field of view is established. Having established the position of the inhibit signal within the field of view and its position within a captured image, a portion of the image relating to a wearer of the inhibitor device is located. This may be done by the pattern recognition algorithm.

A suitable face detection algorithm is disclosed in '*Neural network based face detection*' Rowley, Baluga, Kanade, IEEE PAMI 20(1): pages 23-38. By identifying an image of a host wearer's face, a further image-processing algorithm can be applied to obliterate or obscure details of the person's face. This can be done by reducing the resolution of the image corresponding to the person's face, or by blanking out that portion of the image, or any other like method of obliteration or obscuring the portion of the image.

In one specific implementation, the inhibit message may be carried by an inhibit signal in the form of a physical light, or an infrared light. Such a light may be detectable within captured image, as a high intensity light spot thereby identifying within the image, a position of a wearer of the inhibitor device. In this implementation, there is relied upon a line of sight view between the inhibitor device, and the image capture device.

In other implementations, the inhibitor device may send an ultrasonic signal, or a radio frequency signal or a microwave signal, in which case a line of sight between the image capture device and the inhibitor device is not essential, but a receiver device is required on the image capture device, to detect the inhibitor device, and the problem of locating a position of the inhibitor device within a captured image needs to be addressed.

Referring to Fig. 2 herein there is illustrated schematically a -3dB level 200 of a signal transmitted by an inhibitor device 201. There is also shown an image capture device 202 having a receiver having an omni-directional -3dB level 203. Since the inhibitor device transmits omni-directionally and the image capture device receives an inhibit message with an omni-directional receive beam, whenever the inhibitor device is within close enough range of the image capture device to receive the inhibit message, the image capture device is inhibited.

However, in other implementations, the image capture device and/or the inhibitor device may have a directional response for sending or receiving an inhibit message.

5 Referring to Fig. 3 herein, there is illustrated schematically an inhibitor device having an omni-directional beam represented by a -3dB power level 301, and an image capture device 302 having a directional receive beam represented by a -3dB level 303. When the image capture device is pointing in a direction of the inhibitor device, and is within range of being able to capture and recognize an
10 inhibit message transmitted by the inhibitor device, then the image capture device is inhibited according to the modes described herein above.

Referring to Fig. 4 herein, there is illustrated schematically the image capture device and inhibitor device of Fig. 3, where the image capture device
15 points away from the inhibitor device. Because a receive beam of the image capture device is directional, although the image capture device and inhibitor device may be in relatively close proximity, because the image capture device points away from the inhibitor device, the image capture device is not inhibited.

20 In this implementation, the directional beam of the image capture device coincides with a field of view of image capture, such that when the image capture device is pointing in a particular direction for capturing an image of a scene, the receive beam of the image capture device coincides with the field of view. Signals from inhibitor devices which are outside the field of view of the image capture
25 device, may not be acted upon by the image capture device, so that the image capture device is not inhibited by inhibitor devices outside the field of view.

Referring to Fig. 5 herein, there is illustrated schematically an example of first and second inhibitor devices, 500, 501 respectively, worn by first and second
30 persons (not shown) facing opposite each other. There is also shown an image capture device 502 held or worn by a third person, and in the vicinity of the first and second persons.

Each inhibitor device 500, 501 respectively has a corresponding omni-directional antenna which produces a transmit beam having a corresponding – 3dB level 503, 504 respectively. Image capture device 502 has a receiver having
5 a plurality of directional receive beams 505 to 509, pointing in different directions from each other relative to a primary look direction 510 of the image capture device, along which a center of a field of view of the image capture device lies.

The plurality of directional beams 505 to 509 enable the image capture
10 device to distinguish between the first and second inhibitor devices 500, 501 within a field of view of the image capture device, identified as being between the extremities 511, 512. The first inhibitor device 500 is received upon a central beam 507 and a first left beam 506 of the image capture device, whilst a second inhibitor message from a second inhibitor device 501 is received on the main
15 beam 507 and a first right beam 508.

However if an operator of the image capture device swings the image capture device so that the field of view points towards the inhibitor device, then the directional receive beam of the image capture device receives a signal from
20 an inhibitor device, and the image capture device is inhibited according to the above described inhibited modes.

Referring to Figs. 6 and 7 herein, data processing steps carried out by an image capture device in a second mode of operation will now be described.
25

Figure 6 shows a captured still image of a scene in which a primary subject of the image is a violinist. However, because the image is captured in a public place, a restaurant in this case, in the background of the scene image are images of two other individual persons.
30

A person capturing the image using an image capture device may have no interest in the two diners in the background. However, in the absence of any

mechanism for protection against capture of their images the two diners have no choice but to be included in the image scene. The person capturing the image may use the image for their own purposes, which may include putting the image publicly in the internet, or otherwise publishing the image. This may occur unknown to the two persons who's images exist in the background of the scene image. The persons included in the background of the image may have objected to their inclusion in the image, if they had known the image had been captured.

Referring to Fig. 7 herein, there is shown the same image scene, after data processing by an image capture device as described herein, where the image capture device has received inhibit messages from each of the diners in the background of the image scene, each of whom may be wearing an inhibitor device as described herein.

The image capture device receives two inhibit messages, one from each inhibitor device, worn by each of the diners, and in response to each inhibit message, identifies a person wearing the corresponding inhibitor device. The image capture device processes each frame of image data, to identify images of individual wearers of the inhibitor devices, and then applies data processing to obliterate or remove portions of the image relating to the individual wearers of the inhibitor devices.

Correlation of an inhibit signal to a person in an image can be done in several ways. According to one embodiment, using face-recognition software (known per se), the face nearest to the perceived origin of the inhibitor signal is located in a reference frame defined by the image, and mosaicing the located face.

As shown in Fig. 7, this results in a blurring of the faces of each of the diners in the resultant image frame, thereby protecting the identity and privacy of each of those persons.

A portion of the image scene corresponding to a persons face or other features of the person may be inhibited by obscuring, restricting usage of, replacing and/or deleting the part of the image by various methods including, but not limited to the following:

5

Firstly, a decrease in resolution of the image portion can be applied, so that facial features become blurred and difficult for a human eye to resolve with accuracy. This may be achieved by a digital filtering algorithm, which applies a decrease in resolution to the image portion corresponding to a feature of a person.

10

Secondly, having identified a portion of the image by a known algorithm for detecting skin tone colours within the image scene, the portion of the image corresponding to a persons face may be obscured by overlaying a pre-determined graphic on that portion of the image, so as to obscure or obliterate facial features or other body features of the person.

15

Thirdly, a portion of the image scene corresponding to a person's face or other body features can be de-focused so that it is difficult visually for a viewer to resolve the image with any detail.

20

Fourthly, the image portion corresponding to the person's face or other body features may be obscured by changing an intensity level of the image portion. Typically, the image portion may be darkened so as to cause obscuration of facial features.

25

Fifthly, that portion of the image may be deleted completely, and replaced with a different image, such as a duplicate of another adjacent portion of the image scene. For example in the image shown in Figs. 6 and 7 herein, a portion of the image scene corresponding to a persons face may be identified and removed from the image scene. The resulting gap in the image may be replaced by selecting an adjacent portion of the image scene, for example a background

30

wall, and overlaying this on the gap of the image produced by removal of the image portion corresponding to the persons facial features or other body features. This may have the advantage of retaining similar colouring as adjacent portions of the image.

5

Referring to Fig. 8 herein there is illustrated components of an inhibitor device 800. The inhibitor device comprises a casing 801 shown schematically containing battery, and of a size and shape such that it is easily worn by a person, or can be easily carried by a person, for example in the persons pocket;
10 within the casing, an inhibit message generator 802 for generating one or a plurality of inhibit message types; a transmitter device 803 for transmitting one or more inhibit messages on a carrier signal; an antenna 804 which may generate an omni-directional transmit beam or one or a plurality of directional transmit beams; and a set of user controls 805 for enabling a person to turn the inhibitor
15 device on or off, and optionally for selecting an inhibit message type.

The inhibitor device may also comprise a memory device capable of storing a plurality of images of a persons face, in a plurality of views or orientations, and may be capable of transmitting them images either in encoded or in un-encoded
20 format.

Referring to Fig. 9 herein there is illustrated schematically components of an image capture device 900. The image capture device comprises a casing 901 containing a battery or other power supply; an antenna 902 for receiving inhibit
25 messages, the antenna either having an omni-directional receive beam, or one or a plurality of direction receive beams; a receiver device 903 for receiving a signal from the antenna and amplifying and digitalising the signal; a direction finder 904 for identifying a direction from which an inhibit signal has been received, that is, for identifying from which one or more of a set of directional beams, an inhibit
30 signal was received on; a message recognizer 905 for extracting inhibit messages from received signals and interpreting a type of inhibit message received; a set of optics 906 for capturing an image in response to a user input

signal; an imaging device 907 for converting a received light image into 2 dimensional image data as one or more image data frames, including still images and/or video sequences of a plurality of image frames; an image memory 908 for processing image data frames; an image data storage device 909 for storing
5 captured images; an image processor 910 for applying data processing to captured image data frames; a set of user controls 911 for controlling capture of images via the imaging device 907, and for controlling other functions such as storage of images in the image data store 909, and for monitoring image processing of image data; and an image viewer 912, for example a liquid crystal
10 display (LCD) or the like, for viewing captured images. The antenna, receiver, direction finder, message recognizer and image processor constitute an image inhibitor module 913.

The signal transmitted by the inhibitor device may comprise a visual signal,
15 for example a red coloured visual signal emitted by a light emitting device at a wave length of approximately 633nm, or a green light emitted by an LED at a wave length of approximately 510nm, or may comprise an infrared signal or a microwave or RF frequency signal.

20 In various alternative implementations, signal detector 901 and receiver 903 may comprise an optical detector, such as a photo diode, for detecting visual or infrared signals; an ultrasonic detector for detecting ultrasonic signals, or an antenna for detecting radio frequency signals.

25 Registration of inhibitor devices.

In a further modification of the image capture system described herein, individual inhibitor devices may be registered with individual image capture devices, so as to override the normal inhibitor function of the inhibitor device with
30 respect to those particular registered image capture devices. This function may be useful in situations where inhibitor devices are worn by members of a family group, and one or more other members of the family group are carrying an image

capture device. Persons within the family group may wish to allow image capture by their own family member, but prohibit capture of their images by other unknown third parties in a public place.

5 Referring to Fig. 10 herein, there is illustrated schematically an implementation of an image capture system, in which a plurality of inhibitor devices are pre-registered with one or more image capture devices, and in which the image capture device can ignore an inhibitor message emanating from a pre-registered inhibitor device. An image capture device 1000 receives first and
10 second inhibitor message 1001, 1002 from first and second inhibitor devices 1003, 1004 respectively within a field of view of the image capture device. First inhibitor device 1003 sends an inhibitor message 1001 which contains a code which the image capture device recognises as denoting a known pre-registered inhibitor device. On the other hand, second inhibitor device 1004 sends a signal
15 which is not recognised by the image capture device.

Referring to Fig. 11 herein, there is illustrated processes carried out by the image capture device upon receiving an inhibit message, for checking whether the inhibit message relates to a pre-registered inhibitor device. In process 1100,
20 the image capture device receives an inhibit message. The message is read, and checked for an identification code in process 1101. If the identification code is recognised as one which is pre-registered with the image capture device in process 1102, the image capture device ignores the inhibit message 1103 and takes no action to process parts of a captured image identified by the existence
25 of the inhibit message. In other words, no modification of that part of the image is made. However, if the identification code is not recognised as one which is pre-registered with the image capture device in process 1104, the image capture device continues to restrict a portion of the image corresponding to the inhibit message in process 1104.

30

Consequently, for an image in a field of view where a plurality of inhibitor devices are present, some of which are recognised by the image capture device

and some of which are not, the image capture device operates to modify portions of the image corresponding to inhibitor devices which are not recognised, and leave un-modified portions of the image corresponding to inhibitor devices which have a recognised code.

5

Widespread usage of inhibitor devices may affect security cameras used in surveillance systems. In an environment such as a building society, bank, shop, petrol filling station or the like public place, which are susceptible to criminal activity, criminals wearing inhibitor devices may inhibit a security camera to obscure details of the wearers faces. Therefore, in a further implementation there is provided a facility whereby an inhibit signal received by an image capture device can be overridden so that faces of wearers can be viewed. There are two main options for overriding the inhibit signal, that is (a) without the wearers permission; and (b) with the wearers permission.

15

For a system where the inhibit signal can be overridden without the wearers permission, this can be provided as a function built into the image capture device itself. However, building in such a function seriously compromises the privacy of wearers of inhibitor devices. In a more sophisticated implementation, an operator of an image capture device may be able to override an inhibit signal, only with permission of a trusted third party. In such a system, an operator of an image capture system may send an image to a trusted third party, having the modified image portions corresponding to a persons face, along with a request to reverse the obliteration of a specific persons facial features.

25

Referring to Fig. 12 herein, there is illustrated schematically a signal processing channel within an image capture device for storing a captured scene image in such a way that the image can only be viewed, stored or printed with personal details obscured of persons wearing inhibitor devices, but with a capability to obtain a clear image of those persons with external authorisation from a third party.

30

In process 1200, an image scene is captured, along with an inhibit signal in process 1201. In process 1202, a portion of the scene image is identified which is restricted by the inhibit signal and in process 1203 the identified portion of the image is encoded and stored in an encoded format in process 1204 the encoding
5 may include encryption, and may include protection with an encoding key. Therefore, inhibited portions of the image can only be stored in an encrypted format under protection of an encryption key.

In process 1205, the scene image is processed so that inhibited portions of
10 the scene are obscured or obliterated. The processed scene image, having portions of the image obliterated or obscured can be stored in process 1206, and/or can be made available for viewing or printing in process 1207.

Referring to Fig.13 herein, there is illustrated schematically communication
15 between an image capture device 1300 and a trusted third party computer 1301 over a communications network, for example the internet, in which an encoded image portion is sent to a trusted authority for decoding, so that images of persons can be recovered from the encoded stored image portions under control of a trusted authority. When an operator of the image capture system wishes to
20 obtain a clear image of a particular person who has inhibited capture of their own image using an inhibitor device, they can only do so provided the trusted authority agrees to authorise production of a clear image portion of that persons face. The operator of the image capture device cannot bypass the trusted authority, since the stored image portions are encrypted, and can only be decrypted with a key
25 available to the trusted authority.

Several further variations on the implementations described herein may be incorporated as follows.

30 Referring to Fig. 14 herein, there is illustrated schematically an inhibitor device 1600 and an image capture device 1601, and a remote trusted third party computer 1602, in which the inhibitor device sends an image of a host wearer

either to the image inhibitor module within the image capture device 1601, and/or to a trusted third party computer 1602. The image of the host wearer of the inhibitor device can be sent either as a clear un-encoded image, or it can be sent as an encoded image, in order to prevent mis-appropriation of the image when it is being transmitted between the inhibitor device and the image capture device, or between the inhibitor device and the trusted third party computer.

Operation of the second image capture system as described in Fig. 14 is as follows. Image capture device 1601 is used to capture an image of a scene in a field of view of the image capture device. Within that scene, there may be one or more inhibitor devices 1600. The inhibitor devices announce their presence within the field of view to the image capture device, by a recognition signal, which may comprise the inhibitor message as described previously with respect to the first implementation. However, in addition to that message, the inhibitor device may send to the image capture device an image of the host wearer, thereby enabling the image capture device to match that received image, with a portion of the image captured by the image capture device, which corresponds to a host wearer of the inhibitor device. Matching of the host wearer image received from the inhibitor device with a portion of the image scene captured by the image capture device can be carried out by pattern matching or pattern recognition algorithms which match the host wearers facial image, with portions of the captured image scene in order to detect a match of profiles.

The image sent from the inhibitor device to the image capture device may comprise several views of the host wearers face, so that the face can be recognised from a variety of different angles of view.

In a further mode of operation of the second implementation, the image(s) of the host wearers face may be sent to a trusted third party computer 1602 operated by an independent authority having responsibility for decoding portions of an image. The trusted third party computer 1602 may use the host wearers image in order to recognize portions of a scene image which have been sent to it

by an image capture device 1601, for the purpose of decoding that part of the image as described previously with respect of the first implementation described herein. In this mode of operation, which may have application for obtaining decoding of images taken by a security camera, the operator of the image capture device must obtain authorization for the authority to decode a portion of the image. The trusted third party computer 1602 may use the image of the host wearer received from the image capture device worn by the host wearer to allow decoding of an obliterated or modified portion of the scene image corresponding to the wearers face, so that the operator of the image capture device 1601 can obtain from the trusted third party, a clear image of the host wearers face.

Activation of the Image Inhibitor Module.

In a further variation of the implementations described herein, activation of an image inhibitor device may depend upon either a distance between an image capture device and an inhibitor device, or an effective resolution of an image which the image capture device can capture.

In the first case, an inhibitor device and/or an image capture device are provided with a known distance measuring device, for example a laser based, or diode based measuring system as known in the art. An image capture device may measure a distance between itself and an inhibitor device within a field of view of the image capture device, and depending upon a result of the measurement, the image inhibitor module comprising the image capture device is activated or de-activated. For inhibitor devices which are beyond a pre-specified range the image inhibitor module may be deactivated, allowing the image capture device to store, print or display a scene image including an un-modified image of a host wearers face. Provided that the pre-specified distance is set correctly, the person will be so far in the distance, that they will appear only as a small feature in the captured image, and it may be difficult for persons examining that image to recognise the wearer of the inhibitor device due to their relatively small size as a proportion of the whole of the scene image.

In the second case, the image inhibitor module may not apply modification to any image portions where facial features may not be recognised due to the low resolution of the facial features. For example, this may be because the wearer of an inhibitor device is so far away from the image capture device within a field of view of that device that their facial features cannot be captured with any significantly high resolution such as to enable a person to recognise the wearer of the inhibitor device.

In a further variation, the inhibitor device worn by a person, may be provided in a same casing as an image capture device, to provide an image capture device performing a dual role of enabling a person to capture images of a scene, and at the same time providing a degree of privacy to that person from having their image captured by other image capture devices. For example, the inhibitor device, and an image capture device having an image inhibitor module, may be incorporated in a single hand held device, for example a mobile phone, or still image camera, or hand held video camera device.

In a further variation, within the image capture system, individual security groups or levels of security may be implicitly or explicitly used to ensure if a person carries an inhibitor device, it will still be possible for an authorised person, for example a family member, to be able to capture an image of the wearer of the inhibitor device.

By combining an inhibit message or inhibit signal, with pattern recognition of facial features, that is, by comparing an image sent by the inhibitor device with portions of a scene image, a portion of a scene image relating to a wearers face can be more accurately adjusted and finally located, and modified so as to obscure the facial details of that person.

Specific implementations disclosed herein provide that a person who does not want their image to be captured can carry a portable device to communicate

with one or more image capture devices such as camera's which that person may encounter, to inhibit those image capture devices from using images of the person. The image capture system is de-centralised, and need not rely upon a centralised database of images of person's faces.

Claims:

1. A method for modifying a captured image of a scene, said method comprising:

5 detecting an inhibit signal emanating from an inhibitor device carried by a person within said image;

10 in response to said inhibit signal identifying a portion of said image corresponding to said person; and

modifying said image of said scene to render the person unidentifiable from the modified image.

15 2. The method as claimed in claim 1, wherein identifying a portion of said image corresponding to said person comprises:

locating a source of said inhibit signal within said image of said scene.

20 3. The method as claimed in claim 1, comprising:

identifying a region of said image of said scene in which said image portion corresponding to said person is positioned, by identifying a position of said captured image corresponding to a source of said inhibit signal.

25 4. The method as claimed in claim 1, wherein identifying a portion of said image corresponding to said person comprises:

30 searching said image of said scene for a relatively higher intensity light spot corresponding to said inhibit signal.

5. The method as claimed in claim 1, wherein said step of identifying a portion of said image corresponding to said person comprises:

detecting a skin tone detail within said image of said scene.

5

6. The method as claimed in claim 1, wherein identifying a portion of said image corresponding to said person comprises:

recognizing an outline of said person within said image of said scene.

10

7. The method as claimed in claim 1, wherein identifying a portion of said image corresponding to said person comprises:

15 applying a facial recognition algorithm to said image of said scene, in order to recognize a portion of said image corresponding to a face of said person.

8. The method as claimed in claim 1, wherein modifying said image of said scene so as to obscure said image portion of said person comprises:

20

applying a decrease in resolution to said image portion of said person.

9. The method as claimed in claim 1, wherein modifying said image of said scene so as to obscure said image portion of said person comprises:

25

overlaying a graphic image on said image portion.

10. The method as claimed in claim 1, wherein modifying said image of said scene to obscure said image portion of said person comprises:

30

defocusing said image portion of said person.

11. The method as claimed in claim 1, wherein modifying said image of said scene so as to obscure said image portions said person comprises:

darkening said image portion of said person.

5

12. A user portable inhibitor device capable of transmitting an inhibitor message for inhibiting an image capture device from processing a portion of said image corresponding to a user of said user portable inhibitor device.

10

13. The user portable device as claimed in claim 12, wherein said inhibitor device transmits said inhibitor message directionally.

14. The user portable device as claimed in claim 12, wherein said inhibitor device transmits said inhibitor signal omni-directionally.

15

15. The user portable device as claimed in claim 12, wherein said inhibitor message comprises an infrared signal.

20

16. The user portable device as claimed in claim 12, wherein said inhibitor message comprises a visual signal;

17. The user portable device as claimed in claim 12, wherein said inhibitor message comprises a radio frequency signal.

25

18. An image modifier comprising:

means for identifying an image of at least one person within an image of a scene;

30

means for determining whether the image of said at least one person should be excluded from scene image; and

means for modifying said scene image so as to obscure said image of said at least one person.

5 19. A method for restricting usage of an image of a host person, said method comprising:

transmitting an inhibitor signal from a position close to a body of said host person;

10

receiving said inhibitor signal at an image capture device within a view of said host wearer person; and

15

in response to receiving said inhibitor signal applying a restriction on a captured image of said host wearer, captured by said image capture device.

20. An image capture device comprising:

an imaging system for capturing image data;

20

an image inhibitor module capable of receiving an inhibitor message;

25

an image processor adapted to select portions of said captured image relating to inhibited matter, and modify said inhibited matter portions of said image, so as to obscure said inhibited matter.

21. A method for processing a captured image of a scene, said method comprising:

30

receiving an inhibit signal for inhibiting processing of a portion of said scene image;

identifying a portion of said scene image to which said inhibit message relates; and

5 processing said identified portion of said scene image so as to inhibit viewing of said identified image portion.

22. The method as claimed in claim 21, wherein said inhibit signal is received from a position within a field of view of said scene image.

10 23. The method as claimed in claim 21, wherein said inhibit message comprises a region of relatively high intensity lights within said scene image.

24. The method as claimed in claim 21, further comprising:

15 searching for an inhibit message within said scene image;

searching for a portion of inhibited matter within said scene image, adjacent said inhibit message;

20 processing said region of inhibited matter in said scene image, so as to obscure said inhibited matter from view.

25. An image capture system comprising:

25 an inhibitor device capable of being worn by a person, for inhibiting processing of an image of said wearer;

at least one image capture device, said image capture device provided with an image inhibitor component for inhibiting processing of portions of an image
30 captured by said image capture device; and

an encoder for encoding a portion of said image, said image portion corresponding to an image of said host wearer.

5 26. The image capture system as claimed in claim 25, further comprising a trusted third party computer device, said trusted third party computer capable of:

receiving an encoded image portion; and

10 decoding said image portion.

27. The image capture system as claimed in claim 25, further comprising a trusted third party computer device, said trusted third party computer capable of:

15

receiving an encoded image portion; and

decoding said image portion;

20 wherein, said image capture device operates to send said encoded image portion to said trusted third party computer;

said trusted third party computer operates to decode said encoded image portion to produce a clear image of a person; and

25

said trusted third party computer operates to send said decoded clear image to said image capture device.

28. An image capture system comprising:

30

a host wearable inhibitor device, for inhibiting processing of image data corresponding to said host wearer; and

an image capture device comprising an image inhibitor component for restricting processing of image data corresponding to one or more persons within a captured scene image;

5

wherein, said inhibitor device is operable for sending at least one image of a host wearer of said inhibitor device to said image capture device, such that said image capture device can use said received image for recognizing an image portion corresponding to said person, within said captured scene image.

10

29. An image capture system comprising:

a user wearable inhibitor device, for inhibiting processing of image data corresponding to said host wearer; and

15

a third party computer entity comprising an image inhibitor component for restricting processing of image data corresponding to one or more persons within a captured image scene;

20

wherein said inhibitor device is operable for sending at least one image of a host wearer of said inhibitor device, to said third party computer entity, such that said third party computer entity can use said received image for recognizing an image portion corresponding to said person, within said captured scene image.

25

30. An image capture device comprising:

an optics system capable of forming an image on a detector; and

30

an image inhibitor operable for receiving externally from said image capture device, an inhibit signal for inhibiting a portion of said captured image, and inhibiting viewing of the portion of the image accordingly.

31. The image capture device as claimed in claim 30, further comprising:

5 a portable inhibitor device, said inhibitor device operable for sending an inhibit message for inhibiting viewing of a portion of said captured image relating to a host wearer of said image capture device.

32. A method for modifying a captured image of a scene, said method
10 comprising:

detecting an inhibitor signal generated from a position within said scene image;

15 using said inhibitor signal for identifying an image portion of at least one person within said scene image;

determining that said image portion of said person should be excluded from
said scene image; and

20

modifying said scene image so as to exclude a detailed said image portion of said at least one person within said captured image of said scene.

33. The method as claimed in claim 32, wherein determining whether
25 said image of said person should be included or excluded comprise:

receiving an inhibit message for inhibiting a portion of said image.

34. The method as claimed in claim 32, wherein identifying an image of
30 at least one person comprises:

locating a source of an inhibitor signal within said scene image; and

applying a facial recognition algorithm to said scene image, in order to recognize a face of said at least one person.

5 35. The method as claimed in claim 32, comprising:

 receiving an inhibit message for inhibiting said image of said at least one person; and

 identifying a region of said scene image in which said image of said at least
10 one person is positioned.

 36. The method as claimed in claim 32, wherein identifying an image of at least one person within said scene image comprises:

15 searching said scene image for a relatively higher intensity light spot corresponding to a said at least one person.

 37. The method as claimed in claim 32, wherein modifying said scene image so as to obscure said image of said at least one person comprises:

20 applying a decrease in resolution to said image of said at least one person.

 38. The method as claimed in claim 32, wherein identifying an image of at least one person comprises:

25 recognizing an outline of said image of said at least one person within said scene image.

30

Abstract

IMAGE CAPTURE METHOD

5 A method for modifying a captured image of a scene, said method comprises: detecting an inhibit signal emanating from an inhibitor device carried by a person within said scene; in response to said inhibit signal; identifying a portion of said image corresponding to said person; and modifying said image of said scene so as to obscure said image portion of said person.

10

Fig. 7

MEMORANDUM
FOR THE RECORD
DATE: 02/21/2007

THIS PAGE BLANK (LSP10)

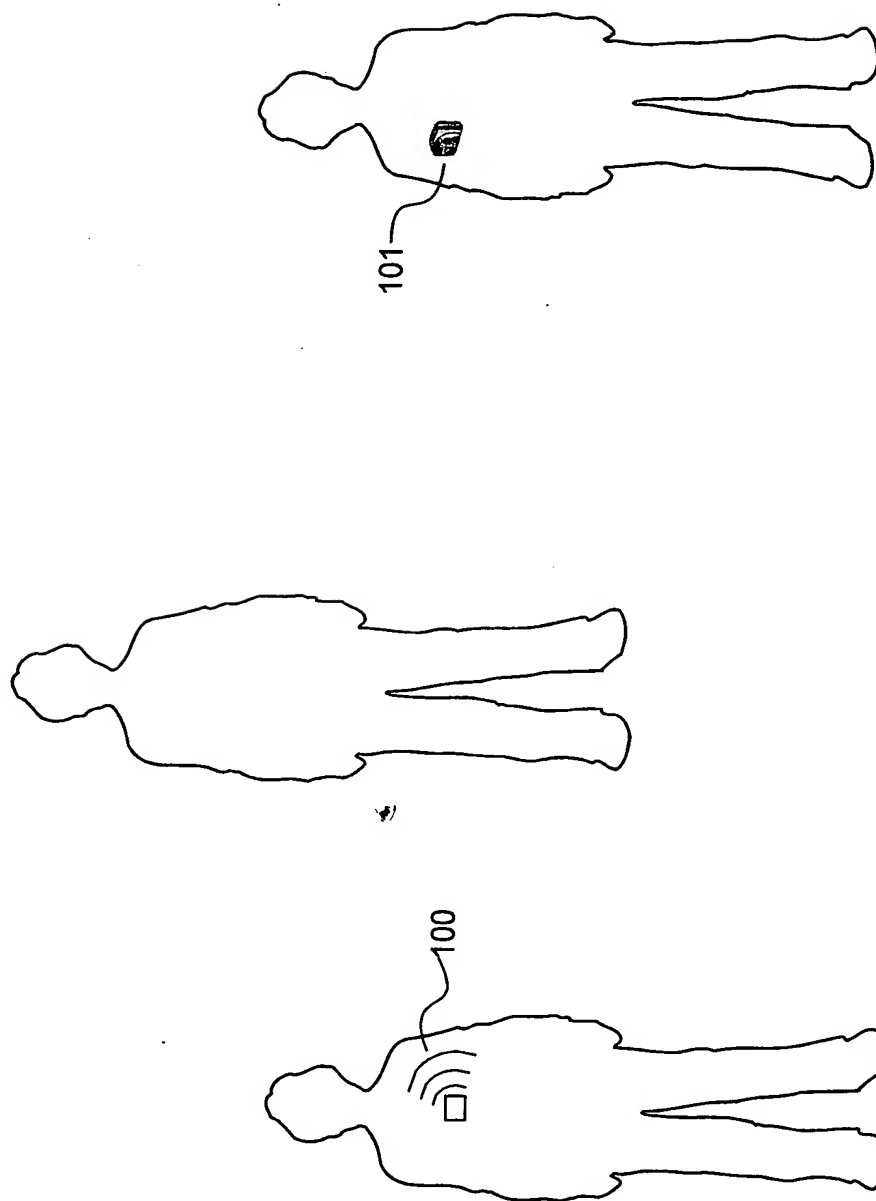


Fig. 1

THIS PAGE BLANK (USPTO)

2/11

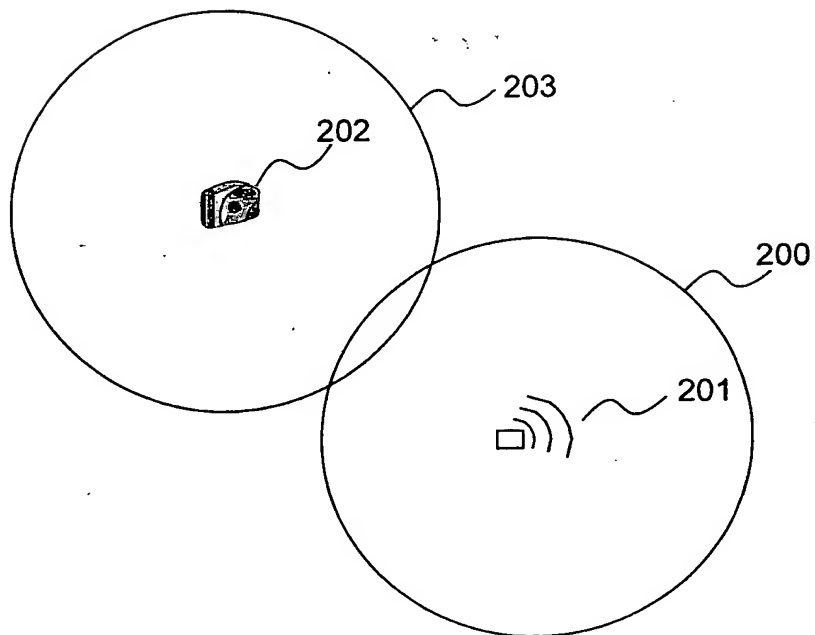


Fig. 2

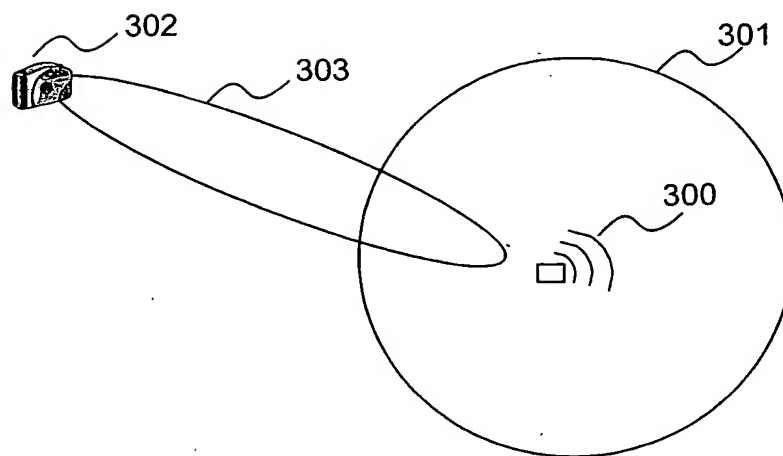


Fig. 3

THIS PAGE BLANK (USPTO)

3/11

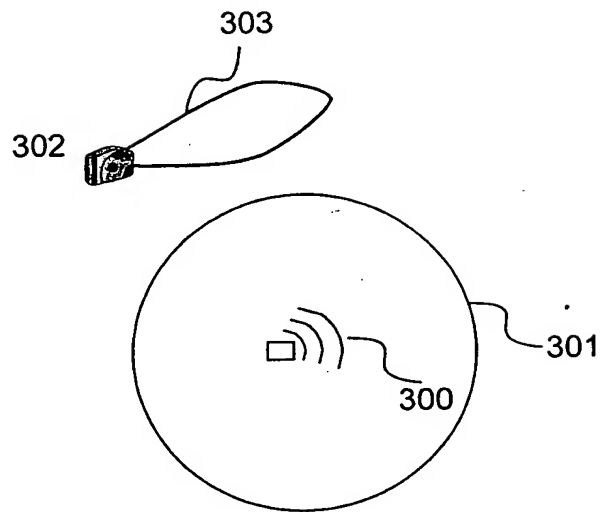


Fig. 4

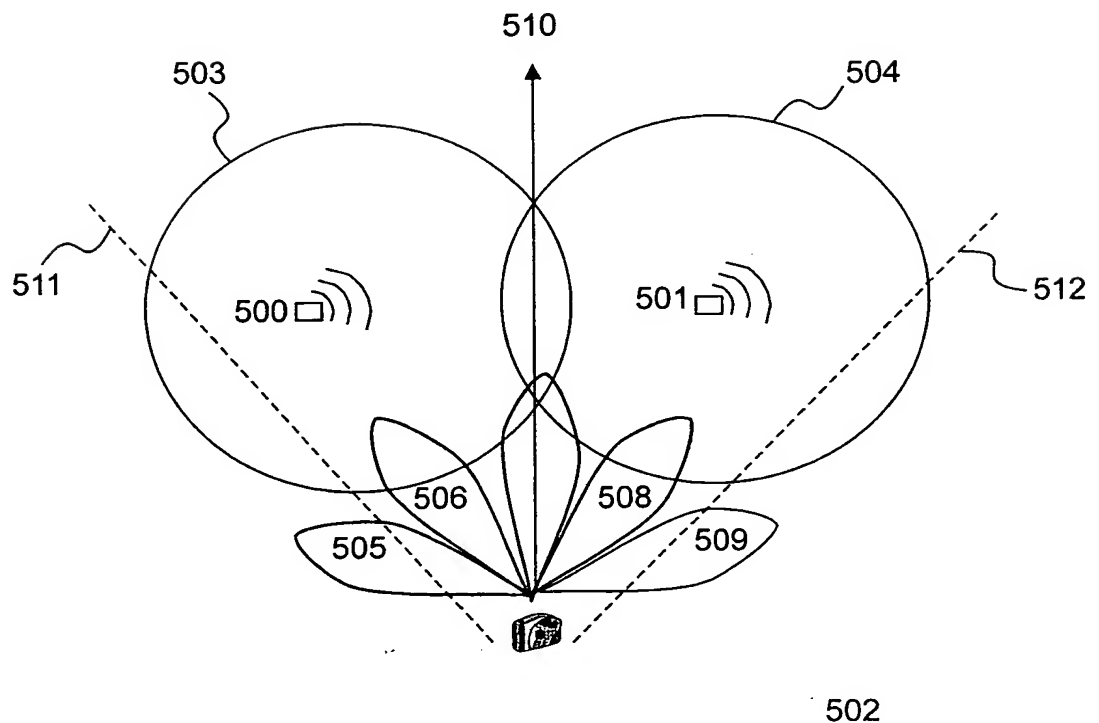


Fig. 5

THIS PAGE BLANK (00PT0)

4/11

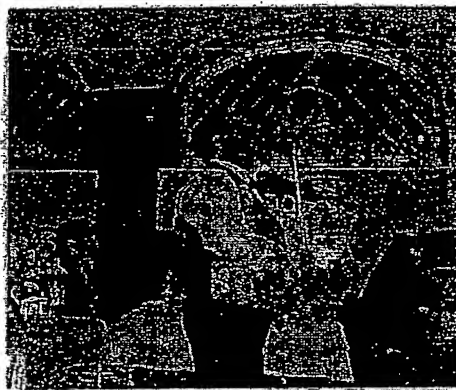


Fig. 6



Fig. 7

THIS PAGE BLANK (USPTO)

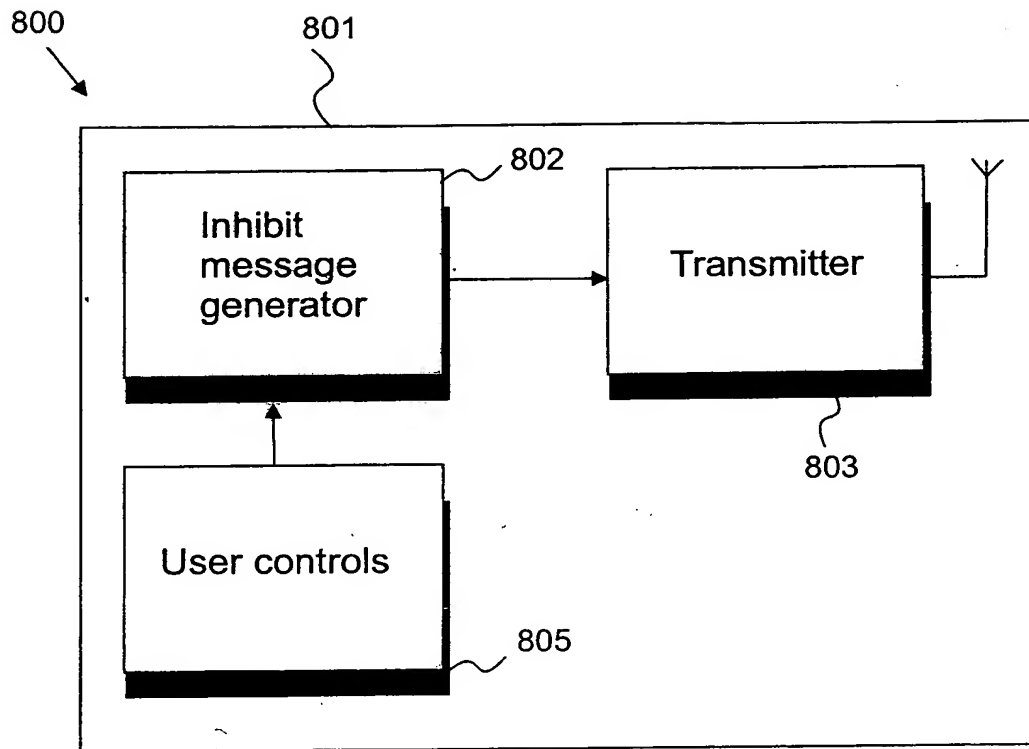


Fig. 8

THIS PAGE BLANK (USPTO)

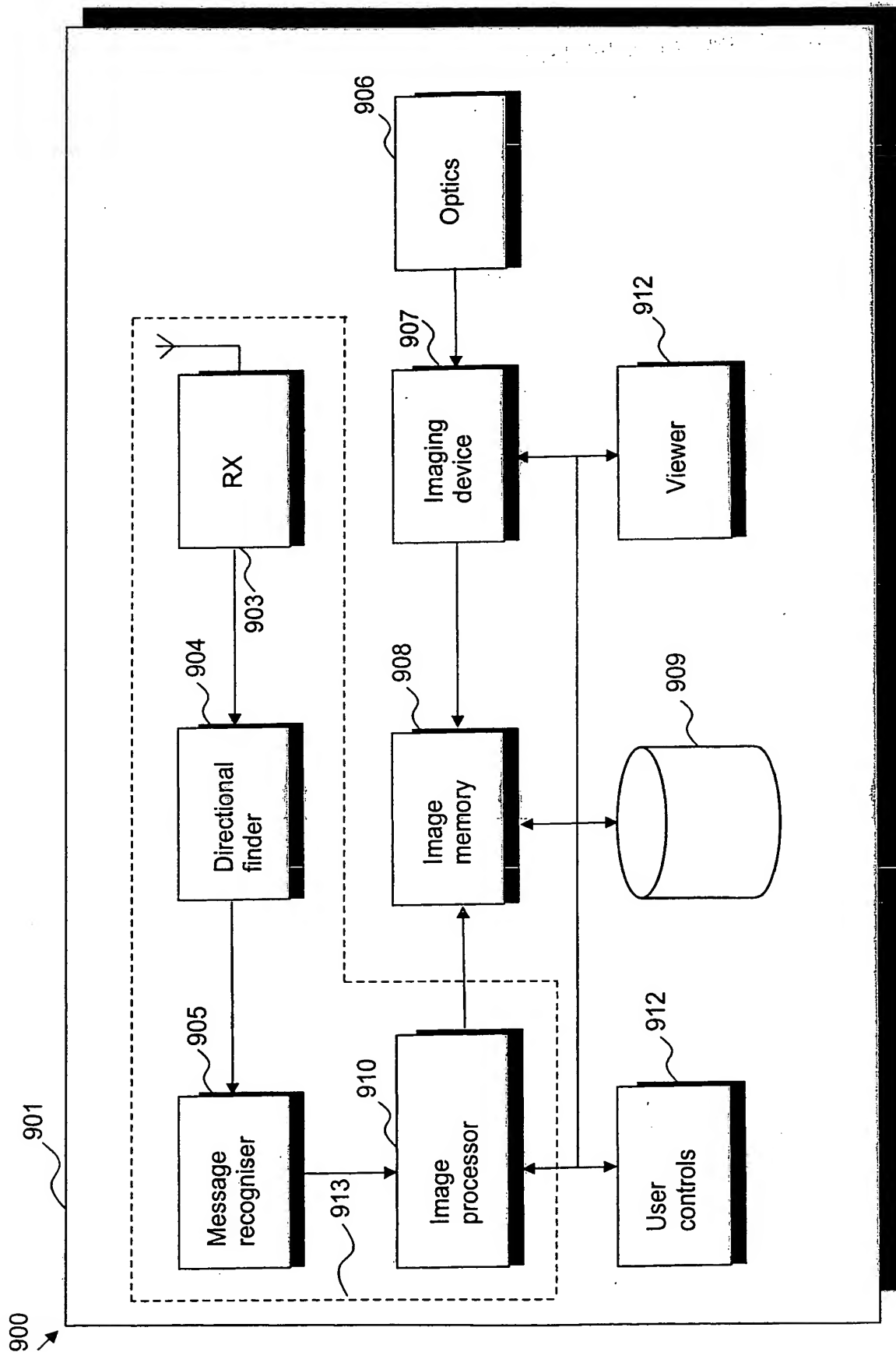


Fig. 9

THIS PAGE BLANK (USPTO)

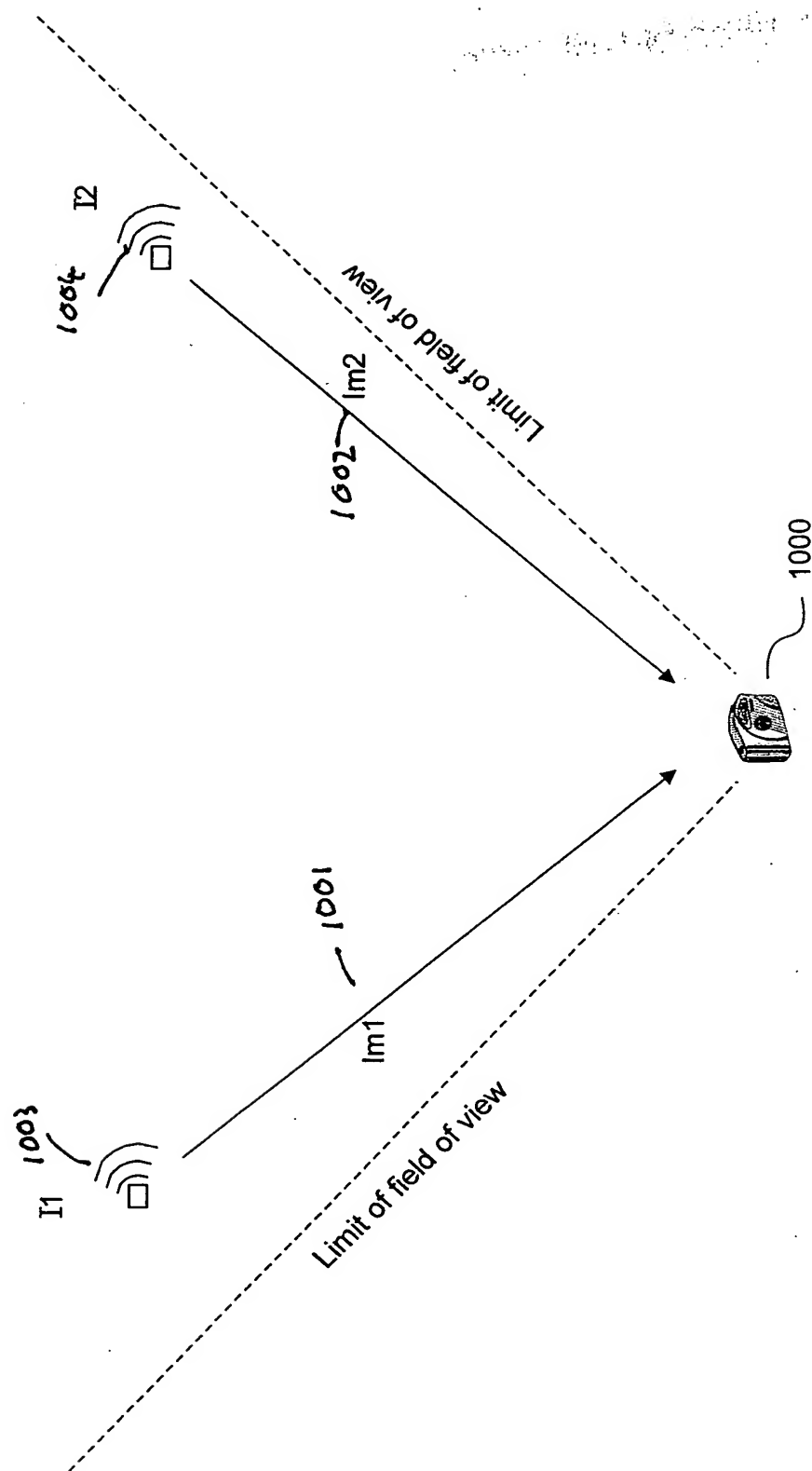


Fig. 10

THIS PAGE BLANK (INFO)

8/11

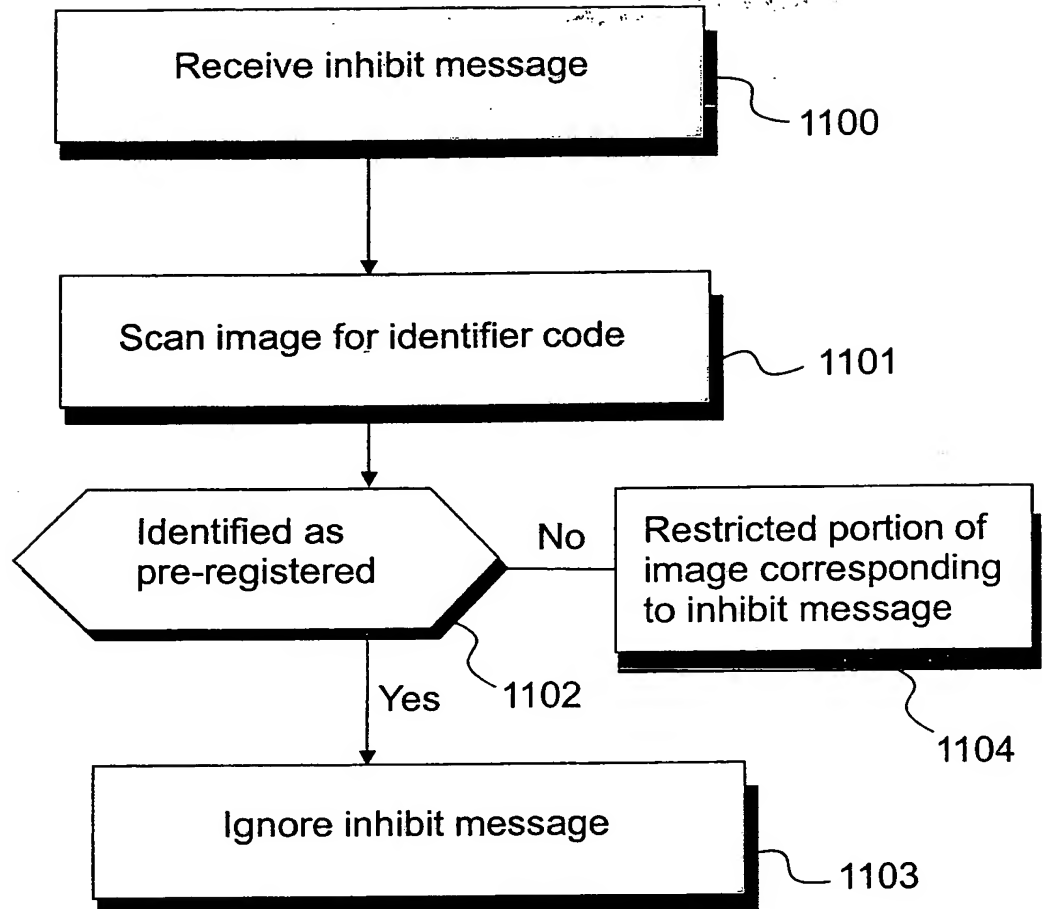


Fig. 11

THIS PAGE BLANK (JSPT0)

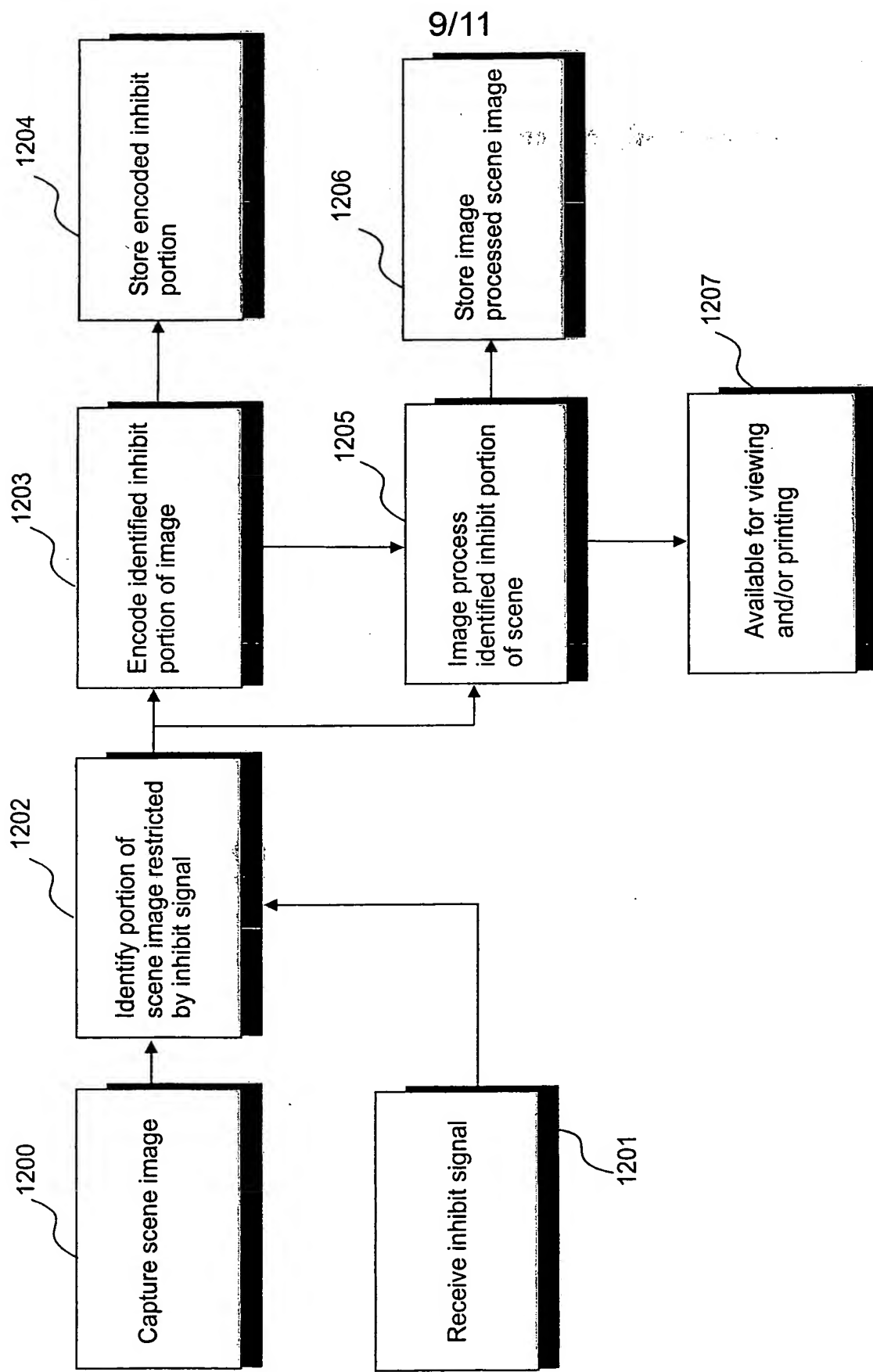


Fig. 12

THIS PAGE BLANK (USPTO)

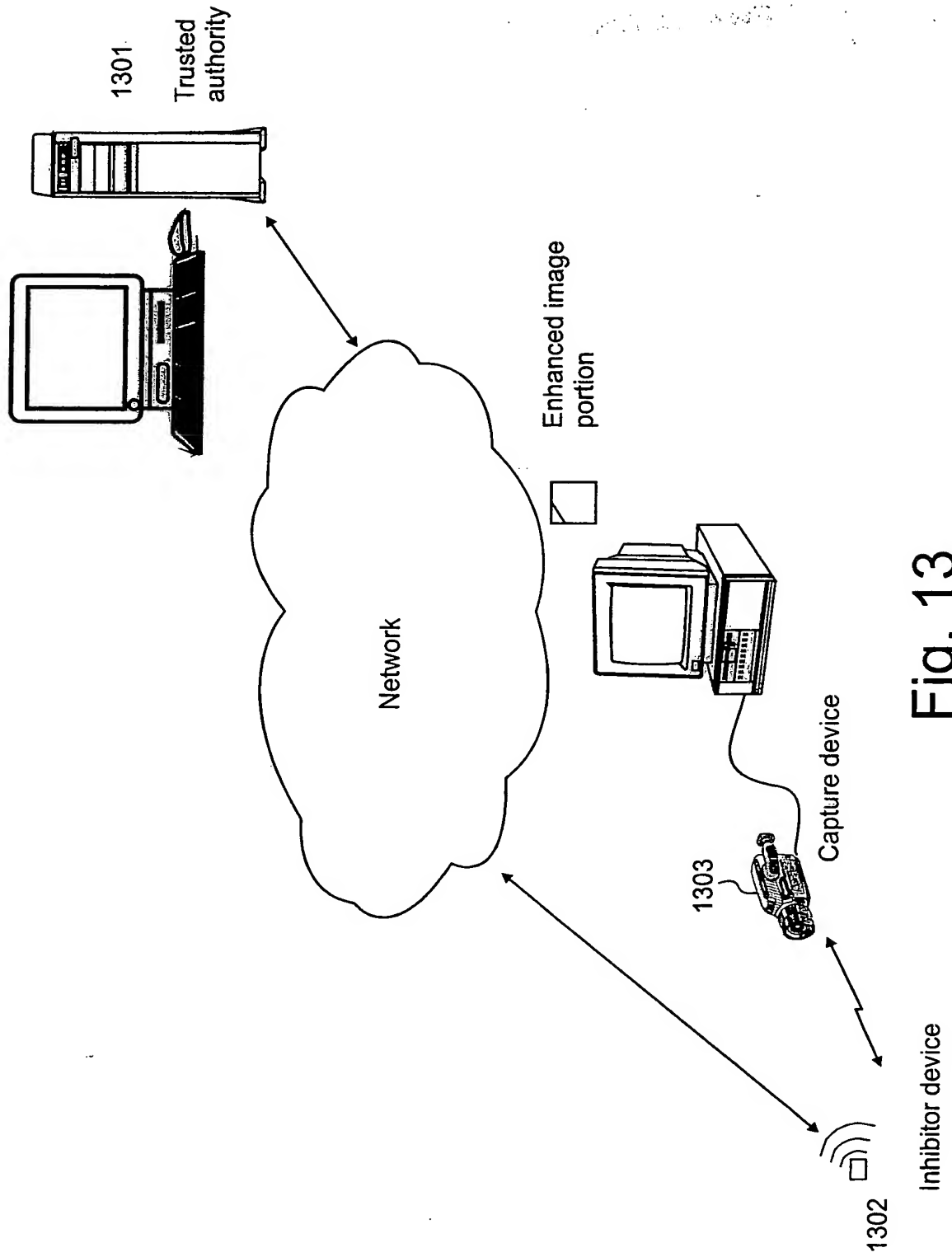


Fig. 13

THIS PAGE BLANK (USPTO)

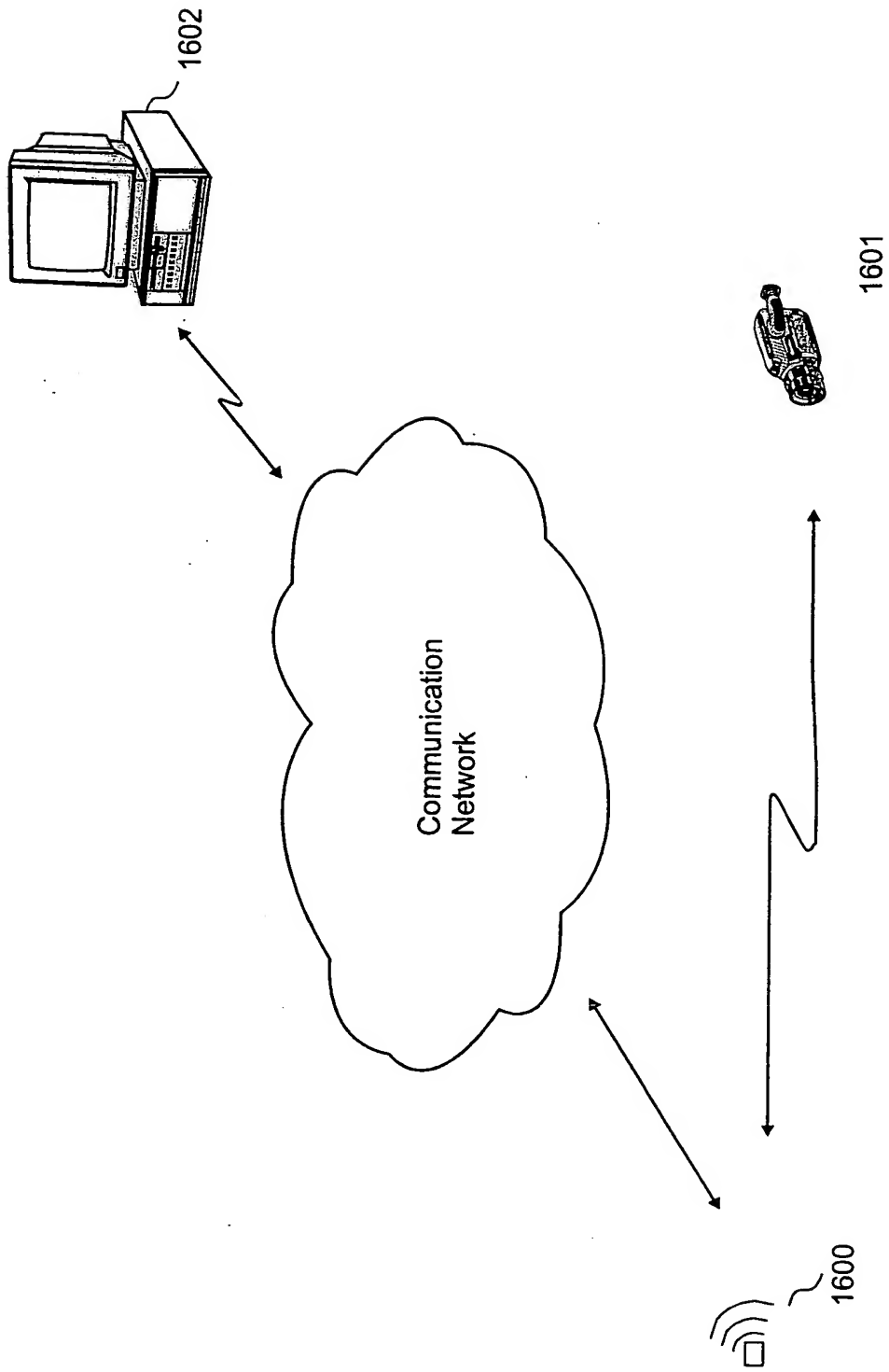


Fig. 14

THIS PAGE BLANK (CSPTO)